

Benjamin Steinberg (admitted *pro hac vice*)
SHINDER CANTOR LERNER LLP
14 Penn Plaza, 19th Floor
New York, NY 10122
Telephone: (646) 960-8601
Facsimile: (646) 960-8625
benjamin@scl-llp.com

Christian Levis (admitted *pro hac vice*)
Margaret MacLean (admitted *pro hac vice*)
Amanda Fiorilla (admitted *pro hac vice*)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Facsimile: (914) 997-0035
clevis@lowey.com
mmaclean@lowey.com
afiorilla@lowey.com

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

DARIUS CLARK, JOHN H. COTTRELL,
DAVID LUMB, KYLA ROLLIER, and
JENNY SZETO, individually and on behalf
of all others similarly situated,

Plaintiff,

v.

YODLEE, INC., a Delaware corporation,

Defendant.

Civil Case No. 3:20-cv-05991-SK

**PLAINTIFFS' OPPOSITION TO YODLEE,
INC.'S REVISED MOTION FOR
SUMMARY JUDGMENT**

Judge: Hon. Sallie Kim
Hearing Date: December 16, 2024
Hearing Time: 9:30 a.m.
Place: Courtroom C – 15th Floor
450 Golden Gate Ave.,
San Francisco, CA 94102

TABLE OF CONTENTS

1	TABLE OF CONTENTS.....	i
2	TABLE OF AUTHORITIES.....	ii
3	I. INTRODUCTION.....	1
4	II. FACTUAL BACKGROUND.....	2
5	A. Yodlee’s IAV Service.....	2
6	B. Yodlee’s IAV Software within PayPal.....	3
7	C. Yodlee Designed the Fake Bank Portal to Mimic a Bank Login.....	5
8	D. Yodlee’s Unnecessary Storage of Plaintiffs’ Data Violated Its Policies and Contracts with PayPal.....	6
9	E. Yodlee Hid Its Conduct from PayPal.....	7
10	F. PayPal’s Policies Did Not Disclose Yodlee’s Conduct.....	9
11	G. Yodlee Collected & Stored Plaintiffs’ Login Credentials and Banking Data.....	10
12	III. LEGAL STANDARD	11
13	IV. ARGUMENT.....	11
14	A. Plaintiffs Have Article III Standing for Each Claim.....	11
15	i. Yodlee’s Collection of Transaction Data Is Irrelevant to Plaintiffs’ Standing.....	12
16	ii. Plaintiffs Lumb and Clark Have Standing	15
17	B. Plaintiffs May Bring Claims Under California Law.....	15
18	C. Plaintiffs’ CAPA Claims Should Proceed	17
19	i. Yodlee Represented Itself as Financial Institutions Without Approval.....	18
20	ii. Plaintiffs Were Adversely Affected under CAPA	19
21	iii. Yodlee Directly Violated CAPA.....	20
22	iv. Plaintiffs Rollier & Szeto’s CAPA Claims Are Not Time-Barred.....	21
23	D. Plaintiffs’ Privacy Claims Should Proceed.....	21
24	i. Yodlee’s Conduct Is Highly Offensive.....	22
25	ii. Yodlee Did Not Obtain Plaintiffs’ Consent.....	23
26	E. Plaintiffs’ Unjust Enrichment Claims Should Proceed.....	25
27	V. CONCLUSION.....	25

TABLE OF AUTHORITIES**Cases**

<i>Brown v. Google LLC</i> , 685 F. Supp. 3d 909 (N.D. Cal. 2023).....	13
<i>Cain v. State Farm Mut. Auto. Ins. Co.</i> , 62 Cal. App. 3d 310 (Cal. Ct. App. 1976).....	21
<i>Cent. Delta Water Agency v. United States</i> , 306 F.3d 938 (9th Cir. 2002).....	11
<i>Chinacast Educ. Corp. v. Chen Zhuoguo</i> , No. CV 15-05475-AB (EX), 2018 WL 6074551 (C.D. Cal. Sept. 7, 2018).....	17
<i>Citizens for Better Forestry v. U.S. Dep't of Agric.</i> , 341 F.3d 961 (9th Cir. 2003).....	19
<i>Cottle v. Plaid Inc.</i> , 536 F. Supp. 3d 461 (N.D. Cal. 2021).....	16, 19
<i>E. Bay Sanctuary Covenant v. Trump</i> , 932 F.3d 742 (9th Cir. 2018).....	19
<i>Eichenberger v. ESPN, Inc.</i> , 876 F.3d 979 (9th Cir. 2017).....	12, 14
<i>Folgelstrom v. Lamps Plus, Inc.</i> , 195 Cal. App. 4th 986 (Cal. Ct. App. 2011).....	23
<i>Fowler v. Univ. of Phoenix, Inc.</i> , 817 F. App'x 442 (9th Cir. 2020).....	21
<i>Goins v. City & Cnty. of San Francisco</i> , 817 F. App'x 442 (9th Cir. 2020).....	11
<i>Golan v. Veritas Entertainment</i> , No. 16-CV-06705, 2018 WL 10455157 (N.D. Cal. Mar. 20, 2018)	24
<i>Hammerling v. Google LLC</i> , No. 22-17024, 2024 WL 937247 (9th Cir. Mar. 5, 2024).....	24
<i>Hammerling v. Google LLC</i> , 615 F. Supp. 3d 1069 (N.D. Cal. 2022).....	23
<i>Hart v. TWC Prod. & Tech. LLC</i> , No. 20-cv03842-JST, 2023 WL 3568078 (N.D. Cal. Mar. 30, 2023).....	24, 25
<i>Heldt v. Guardian Life Ins. Co. of Am.</i> , No. 16-cv-885-BAS-NLS, 2019 WL 651503 (S.D. Cal. Feb. 15, 2019).....	25

1	<i>Hernandez v. Hillsides, Inc.</i> ,	
2	47 Cal. 4th 272 (2009)	23
3	<i>I.C. v. Zynga, Inc.</i> ,	
4	600 F. Supp. 3d 1034 (N.D. Cal. 2022).....	13
5	<i>In re Facebook, Inc. Internet Tracking Litig.</i> ,	
6	956 F.3d 589 (9th Cir. 2020).....	11, 14
7	<i>In re iPhone Application Litig.</i> ,	
8	844 F. Supp. 2d 1040 (N.D. Cal. 2012).....	23
9	<i>In re Yahoo Mail Litig.</i> ,	
10	308 F.R.D. 577 (N.D. Cal. 2015).....	17
11	<i>Javier v. Assurance IQ, LLC</i> ,	
12	No. 4:20-cv-2860-JSW, 2021 WL 940319 (N.D. Cal. Mar. 9, 2021).....	24
13	<i>Jones v. Ford Motor Co.</i> ,	
14	85 F.4th 570 (9th Cir. 2023).....	11, 13
15	<i>Katz-Lacabe v. Oracle Am., Inc.</i> ,	
16	668 F. Supp. 3d 928 (N.D. Cal. 2023).....	16
17	<i>Kniesel v. ESPN</i> ,	
18	393 F.3d 1068 (9th Cir. 2005)	19
19	<i>Lawrence v. Finicity Corp.</i> ,	
20	716 F. Supp. 3d 851 (E.D. Cal. 2024).....	14, 16, 19
21	<i>Lopez v. Contra Costa Reg'l Med. Ctr., No. C</i> ,	
22	12-03726 LB, 2014 WL 4349080 (N.D. Cal. Sept. 2, 2014).....	19, 20
23	<i>Low v. LinkedIn Corp.</i> ,	
24	900 F. Supp. 2d 1010 (N.D. Cal. 2012).....	23
25	<i>Marsicano v. Bank of Am. N.A.</i> ,	
26	2016 WL 10968664 (C.D. Cal. Dec. 19, 2016).....	21
27	<i>Mayfield v. United States</i> ,	
28	599 F.3d 964 (9th Cir. 2010).....	12
	<i>Mazza v. Am. Honda Motor Co., Inc.</i> ,	
	666 F.3d 581 (9th Cir. 2010).....	15, 16
	<i>Nayab v. Cap. One Bank (USA), N.A.</i> ,	
	942 F.3d 480 (9th Cir. 2019).....	11, 12, 22
	<i>Norman-Bloodsaw v. Lawrence Berkeley Lab'y</i> ,	
	135 F.3d 1260 (9th Cir. 1998)	12

1	<i>Opperman v. Path, Inc.</i> ,	
2	205 F. Supp. 3d 1064 (N.D. Cal. 2016).....	22, 23, 24
3	<i>Opperman v. Path, Inc.</i> ,	
4	No. 13-cv-453-JST, 2016 WL 3844326 (N.D. Cal. July 15, 2016).....	15, 16
5	<i>Perkins v. LinkedIn Corp.</i> ,	
6	53 F. Supp. 3d 1190 (N.D. Cal. 2014).....	24
7	<i>Phillips v. U.S. Customs & Border Prot.</i> ,	
8	74 F.4th 986 (9th Cir. 2023).....	12
9	<i>San Diego Cnty. Credit Union v. Citizens Equity First Credit Union</i> ,	
10	No. 18CV967-GPC(MSB), 2020 WL 5797826 (S.D. Cal. Sept. 29, 2020).....	21
11	<i>Sanchez v. Los Angeles Dep't of Transportation</i> ,	
12	39 F.4th 548 (9th Cir. 2022).....	11
13	<i>Silver v. Stripe Inc.</i> ,	
14	No. 4:20-cv-8196-YGR, 2021 WL 3191752 (N.D. Cal. July 28, 2021).....	24
15	<i>SkinMedica, Inc. v. Histogen Inc.</i> ,	
16	869 F. Supp. 2d 1176 (S.D. Cal. 2012).....	21
17	<i>Smith v. Facebook, Inc.</i> ,	
18	262 F. Supp. 3d 943 (N.D. Cal. 2017), <i>aff'd</i> , 745 F. App'x 8 (9th Cir. 2018).....	24
19	<i>Sponchiado v. Apple Inc.</i> ,	
20	No. 18-cv-7533-HSG, 2019 WL 6117482 (N.D. Cal. Nov. 18, 2019).....	19
21	<i>Susan B. Anthony List v. Driehaus</i> ,	
22	573 U.S. 149 (2014).....	13
23	<i>Swafford v. Int'l Bus. Machines Corp.</i> ,	
24	408 F. Supp. 3d 1131 (N.D. Cal. 2019).....	25
25	<i>Taus v. Loftus</i> ,	
26	40 Cal. 4th 683 (2007).....	22
27	<i>TransUnion LLC v. Ramirez</i> ,	
28	594 U.S. 413 (2021).....	11, 13
	<i>United States v. Prasad</i> ,	
	18 F.4th 313 (9th Cir. 2021).....	21
	<i>Van Patten v. Vertical Fitness Group, LLC</i> ,	
	847 F.3d 1037 (9th Cir. 2017).....	23
	<i>Virgil v. Time, Inc.</i> ,	
	527 F.2d 1122 (9th Cir. 1975).....	22

1 *Warner v. Experian Info. Sols., Inc.*,
931 F.3d 917 (9th Cir. 2019)..... 20, 21

2 *Wesch v. Yodlee, Inc.*,
3 No. 20-CV-05991-SK, 2021 WL 1399291 (N.D. Cal. Feb. 16, 2021)..... 21, 22

4 *Yunker v. Pandora Media, Inc.*,
5 No. 11-cv-3113-JSW, 2013 WL 1282980 (N.D. Cal. Mar. 26, 2013)..... 23

6 **Statutes**

7 Cal. Bus. & Prof. Code § 22948.2 17

8 Cal. Bus. & Prof. Code §§ 22948.1-22948.2..... 16, 17

9 **Rules**

10 Fed. R. Civ. P. 56(a)..... 11

11 **Other Authorities**

12 Comm. Rep. CA S.B. 355, 2005 WL 1907987 (Apr. 8, 2005), 13, 14

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

I. INTRODUCTION

Two years ago, Yodlee moved for summary judgment on Plaintiffs' PayPal claims. At the time, Yodlee represented its production of "PayPal documents" was complete and that "Plaintiffs [had] received any PayPal documents that may be relevant to [that] . . . motion[.]" ECF No. 170 at 2; *see also* ECF No. 171. Based on this evidence, the Court largely denied Yodlee's motion, allowing Plaintiffs' invasion of privacy, California Anti-Phishing Act ("CAPA"), and unjust enrichment claims to proceed. *See* Order Regarding Yodlee's Motion for Summary Judgment ("SJ Order"), ECF No. 266.

The limited additional discovery conducted following the SJ Order has not changed the facts underlying the Court's ruling and if anything, confirmed what the Court found in 2022. *See* SJ Order. For instance, the Court originally sustained Plaintiffs' privacy claims because it acknowledged that "examining . . . private bank account[s]" is an invasion of privacy (SJ Order at 16-17) and correctly found that whether posing as consumers' financial institutions, searching all accounts, and storing login credentials and data indefinitely are highly offensive were questions for the jury. *Id.* at 17-18. Now, Yodlee has produced account-linking data and other evidence confirming it did in fact collect Plaintiffs' private bank account credentials ("Login Credentials") through its fake bank portal and used those Login Credentials to rummage through their private bank accounts to collect even *more* private bank data. *See* Section II.B. Discovery also confirms Yodlee stored this data indefinitely, [REDACTED] [REDACTED].¹ *Id.*

Similarly, the Court originally rejected Yodlee's consent defense, finding that PayPal's account-linking screens and "Privacy Statement" presented an "open question for the jury" as to whether "those statements were clear enough to show that Plaintiffs consented to" Yodlee's collection, storage, and use of their private Banking Data. SJ Order at 18-19. This time, Yodlee relies on the *same* inadequate Privacy Statements, as well as PayPal Terms & Conditions ("T&Cs") that were hyperlinked in the account-linking screens only before 2020. These earlier T&Cs, however, are even *more* vague than the Privacy Statements this Court already found insufficient to establish consent. Thus, these "new" documents add nothing, and confirm that Yodlee's consent defense should be rejected a second time.

¹ "Banking Data" refers to bank account number, routing number, account holder name, account name, account type, account balance, and account last updated date. *See infra* note 7.

Likewise, the Court originally sustained CAPA claims holding Plaintiffs were “adversely affected” because “their financial data was taken when Yodlee allegedly mimicked their banks’ websites.” *Id.* at 26. The record now indisputably established Plaintiffs’ Login Credentials and Banking Data were taken by Yodlee, and that the screens presented to each Plaintiff did in fact pose as the “log in” screens for their legitimate financial institutions. There is no reason these claims should be dismissed *now* when they have been further solidified with evidentiary support.

Yodlee’s new arguments fare no better. Its choice of law arguments are inconsistent with the record, which confirms that Yodlee collects Plaintiffs’ Login Credentials on its [REDACTED] and then uses “gatherer” agents running on these same [REDACTED] to log into Plaintiffs’ private accounts and collect additional data. None of these acts occur where Plaintiffs individually reside. Yodlee’s challenge to Plaintiffs’ Article III standing also fails, as it is now indisputable that Yodlee collected and stored Plaintiffs’ Login Credentials and other private Banking Data. This conduct violates CAPA, which protects Plaintiffs’ substantive rights in this “identifying information,” and, separately, constitutes a privacy harm routinely found sufficient for Article III standing. Yodlee’s argument that these violations are not actionable unless Plaintiffs can separately prove that they resulted in a separate, downstream harm from Yodlee’s use of such sensitive Banking Data contradicts decades of controlling Ninth Circuit law. For each of these reasons, Yodlee’s Revised Motion for Summary Judgment (“Motion” or “Mot.”) should be denied a second time. ECF No. 615.

II. FACTUAL BACKGROUND

A. Yodlee’s IAV Service

Yodlee is one of the largest consumer financial data aggregators in the world,² with consumer financial data representing “[t]he core to [its] business model.”³ Yodlee gains access to consumer data primarily through software that it provides to banks and other financial institutions,⁴ such as its Instant Account Verification (“IAV”) service.

Yodlee markets IAV as a way for individuals to verify ownership of a bank account in “real time”

² ECF No. 178-4 at ‘111; ECF No. 178-5 at ‘061.

³ ECF No. 493-5 at ‘164 (email stating “[t]he core to our business model is the ‘data’ element.”).

⁴ ECF No. 178-5 at ‘061 (Yodlee’s “data acquisition capabilities” including its “Account Verification”)

when linking that account to a website or mobile app.⁵ To perform IAV, Yodlee collects users' Login Credentials through a digital interface. *See* Section II.B. After storing users' Login Credentials [REDACTED],⁶ Yodlee logs in to the users' bank website from within California, using software "agents" on those same servers to collect a standard set of Banking Data from every available account.⁷ Yodlee then stores this Banking Data with individuals' Login Credentials on its [REDACTED] indefinitely.⁸

B. Yodlee's IAV Software within PayPal

PayPal has used Yodlee's IAV "data service" since [REDACTED]⁹ and is Yodlee's largest IAV customer.¹⁰ To link bank accounts to PayPal, Yodlee instructs PayPal users to log in to their online bank accounts by entering their bank Login Credentials into what is described as their [REDACTED]. *See* Figures 2-4 below. In reality, this login portal is not connected to any banks, but only to Yodlee, which uses the Login Credentials to access and collect further Banking Data from users' accounts.¹¹

Each Plaintiff linked at least one bank account to PayPal via IAV. Plaintiff Rollier linked her bank account to PayPal via IAV on August 22, 2017; Plaintiff Szeto did so on May 20, 2018; Plaintiff Cottrell

⁵ ECF No. 492-37 at '018.

⁶ Declaration of Christian Levis in Support of Plaintiffs' Opposition to Yodlee's Revised Motion for Summary Judgment ("Levis Decl.") Ex. 1 at '348 [REDACTED]; *id.* at 356 [REDACTED]; Levis Decl. Ex. 2 at '947 ([REDACTED])

[REDACTED] Levis Decl. Ex. 3 at '016 ([REDACTED]).

⁷ ECF No. 492-42 at 2 (Yodlee collected [REDACTED] ECF No. 492-43 at 9 ("[T]he IAV service retrieved bank account data from any deposit account held at the provider selected by the user."); ECF No. 492-12 at '034 (confirming Yodlee "in fact pull[s] back and provide[s] all accounts linked to the FI user provides credentials for."); Levis Decl. Ex. 4 at '178 ([REDACTED] ECF No. 178-43 at 4 (Yodlee's "[a]gents" are "capable of navigating to different web pages and retrieving data to be displayed to the consumer on the partner's website"); *see also supra* note 5.

⁸ ECF No. 178-39 at 197:15-19 (testifying that IAV data retention is "always indefinite"); ECF No. 492-42 at 4 (stating Yodlee only deletes PayPal user data if PayPal "initiate[s] Yodlee's deletion of the IAV user's data through a Yodlee API or Yodlee CRM tool"); *see also supra* note 5.

⁹ *See* ECF No. 492-42 at 2 ([REDACTED]); Levis Decl. Ex. 5 at '211 ([REDACTED])

¹⁰ ECF No. 492-10 at '164; Levis Decl. Ex. 6 at '848 (same)

¹¹ ECF No. 178-59 at '314.

did so on March 11, 2020; Plaintiff Lumb did so on December 21, 2022; and Plaintiff Clark did so on April 9, 2023.¹² As a result, and unbeknownst to Plaintiffs, Yodlee collected each Plaintiff's Login Credentials and Banking Data and stored this information on its California servers indefinitely.¹³ The versions of the false login portal Plaintiffs were shown when linking their bank accounts to PayPal are reflected in Figures 1-4 below.¹⁴ PayPal users who used the Yodlee account linking feature between July 2016 and January 2020, like Rollier and Szeto, were shown the screens in Figures 1-3.¹⁵

FIGURE 1

Select your bank

**FIGURE 2**

Confirm Instantly

Enter your bank info so we can confirm you own the account. We'll never store or share it with anyone.

Citi Bank (online.citibank.com)

 User ID
 Password
 PIN(Optional)

By clicking **Link Bank Instantly**, you agree to the [Terms and Conditions](#) for linking your bank.

Confirm Instantly

No thanks, I'll enter random deposits

FIGURE 3

Bank login

Use your Chase Bank login to link your bank. We don't save this information.

CHASE

By clicking **Link Bank Instantly**, you agree to the [Terms and Conditions](#) for linking your bank.

Link Bank Instantly

or

Enter account number manually instead

FIGURE 4

Start using your bank today

Log in to your online banking to link your account instantly.

Bank of America

Online ID - Bank of America

Passcode - Bank of America

We use Yodlee to confirm your bank details and to check your balance and transactions as needed, which can help your PayPal payments go through. For more information, see our [Privacy Statement](#). You can turn off our use of Yodlee by removing permissions for this bank in your Profile.

Agree and Link

Link your bank another way
(Takes 2-3 business days.)

¹² ECF No. 492-35.

¹³ See No. ECF No. 514-2 (Rollier's data); ECF No. 512-5 (Cottrell's data); ECF No. 512-6 (Lumb's data); ECF No. 581-4 (Clark's data); ECF No. 492-35 (showing Szeto's linkage); *see also supra* note 7.

¹⁴ Yodlee's Figure 1 incorrectly incorporates screens related to the micro deposit account-linking flow. These screens would not have been seen by Plaintiffs because they did not link the accounts at issue through micro deposits. *See* ECF No. 492-35; Levis Decl. Ex. 7.

¹⁵ ECF No. 493-17 at '852 (Figure 1); *id.* at '853 (Figure 3); ECF No. 492-55 at '872 (Figure 2); ECF No. 509-6 ¶ 11 (confirming that the screens depicted in Figures 1-3 were in effect between July 6, 2016 and at least approximately January 2020). If the bank is supported by "Frictionless Add Bank," users see Figure 3. *See id.* If the bank is not supported, users see Figure 2. *Id.*

1 These screens never mention Yodlee. Both screens in Figures 2-3 also unambiguously promise users the
2 data they enter will never be “store[d]” or “save[ed],” even though that is exactly what Yodlee did.¹⁶

3 PayPal users who linked accounts after January 2020, like Cottrell, Lumb, and Clark, were shown
4 the screen in Figure 4.¹⁷ These screens also hid Yodlee’s collection and storage of Login Credentials and
5 Banking Data. Like Figures 2-3, this screen directs PayPal users to “[l]og in” to their “online banking”
6 accounts as if interacting directly with their bank, even though they are dealing with Yodlee. Users are
7 then incorrectly told that Yodlee’s role is limited to “confirm[ing] your bank details . . . as needed” to
8 “help your PayPal payments go through” when in fact Yodlee *collects* and *stores* their Login Credentials
9 and Banking Data *forever*. See Section II.A. There is also no disclosure that Yodlee will *collect* and *store*
10 data from accounts users did not link to PayPal. Further, although the user interface in Figure 4 [REDACTED]

11 [REDACTED]
12 [REDACTED] it omits that this has no impact on the Login Credentials and Banking Data that Yodlee had
13 already collected and stored or that users had no ability to delete this data.¹⁸

14 C. Yodlee Designed the Fake Bank Portal to Mimic a Bank Login

15 Yodlee intentionally designed its user interface to mimic the login portal of a bank website so that
16 users would “feel more secure moving forward”¹⁹ at [REDACTED]

17 [REDACTED]²⁰ To do so, Yodlee surrounded the false login portal with the
18 [REDACTED]

19 ¹⁶ See *supra* note 15; see also ECF No. 492-42 at 4 (explaining Yodlee “stores or previously stored” “all”
20 Banking Data and Login Credentials for PayPal users).

21 ¹⁷ ECF No. 492-34 (Figure 4); ECF No. 509-6 ¶ 14 (confirming that the screen depicted in Figure 4 was
22 in effect after January 2020); see also ECF No. 178-31.

23 ¹⁸ ECF No. 492-42 at 2–4 (Yodlee did not delete the collected IAV data fields until PayPal “initiate[d]”
24 Yodlee’s deletion of the IAV user’s data through a Yodlee API or Yodlee CRM tool”); ECF No. 178-39
25 at 148:5–8 (“Q: So again, then the end user cannot directly delete data from Yodlee’s platform?” “A:
26 Cannot. They cannot.”); *id.* at 147:13-17 (Yodlee’s “customer[s], not the end user[s]” can delete data).

27 ¹⁹ ECF No. 178-36 at ‘100 (Yodlee’s Senior Director of Client Partnerships explaining that including bank
28 logos “helps customers feel that the site they are aggregating was legitimate, and made them feel more
secure moving forward”); *id.* at ‘101 (explaining the logos “add legitimacy to the service” and users “trust”
IAV more when they “see logos.”); ECF No. 492-8 at ‘256 ([REDACTED]); ECF No. 178-36 at ‘100 (explaining customers expect to see the logo when logging in during
“similar experiences, especially with their financial institution”); see also Expert Report of Nathan Good
 (“Good Report”), ECF No. 492-52 at 58–65; ECF No. 492-33; ECF No. 492-54; ECF No. 492-32; ECF
No. 492-53 at ‘862; ECF No. 492-34.

²⁰ ECF No. 492-30 at 7.

banks' name, URLs, and logos without a single bank's authorization.²¹ To further obscure its data practices,

²²

At all relevant times, Yodlee retained control over the user interface implemented by its IAV customers, including PayPal. Although PayPal had certain ²³—it could not make changes on its own.

²⁴ ²⁵

D. Yodlee's Unnecessary Storage of Plaintiffs' Data Violated Its Policies and Contracts with PayPal

Yodlee refers to IAV as a purportedly ²⁶ i.e., that it only accesses a bank account once to verify ownership or to collect the data passed to data service customers like PayPal.²⁷ Because the IAV process supposedly completes after this initial login, there is no need for Yodlee to store users' Login Credentials or Banking Data indefinitely.

This is reflected in

²¹ See, e.g., ECF No. 178-36 at '100 ("Yodlee doesn't have any agreements to use financial institution's logos in FastLink[.]"); ECF No. 178-37 at '363 *see also supra* note 19.

²² ECF No. 492-8 at '259

id. at 11

see also ECF No. 492-47 at 265:1–266:4 (testifying that "Yodlee was never mentioned on any of our customer sites" because "Yodlee . . . didn't push that on [its] customers").

²³ See ECF No. 492-68 (

²⁴ Levis Decl. Ex. 8 at '705

Levis Decl. Ex. 9 at '791

²⁵ Levis Decl. Ex. 10 at '414-16

²⁶ ECF No. 178-37 at '356.

²⁷ ECF No. 492-37 at '020 (stating Yodlee's data service uses the credentials to retrieve "all verification information" from the bank and then "performs the verification"); Levis Decl. Ex. 5 at '211 (Yodlee employee confirming PayPal "uses Data service of the verification product").

²⁸ Yodlee's

²⁹ Employees noted

Yodlee nonetheless stored Plaintiffs' Login Credentials and Banking Data because it was commercially valuable for Yodlee.³¹ For example, Yodlee performed targeted analysis on decrypted PayPal user data "to understand the pattern in IAV data and create rules around it," which helped Yodlee find "more use cases" for IAV.³² ³³ While Yodlee claims PayPal later allowed it to begin storing users' Login Credentials with the launch of its "balance refresh" service in February 2020 (Mot. at 3), this was never disclosed or agreed to by Plaintiffs or PayPal users. *See* Section II.F. Nor was it disclosed to them that Yodlee would use Login Credentials *it already stored* to access PayPal user's bank accounts long after they had linked an account. *Id.* Up until at least the filing of this Action,

³⁴

E. Yodlee Hid Its Conduct from PayPal

Despite promising PayPal it would purge users' Login Credentials and Banking Data within 24 hours, Yodlee secretly retained this data and did not delete it from its system.³⁵ Yodlee ³⁶ For instance,

²⁸ ECF No. 492-19 at '433-35 () (emphasis added).

²⁹ ECF No. 492-38 at '046.

³⁰ ECF No. 178-37 at '356.

³¹ ECF No. 492-40 (explaining Yodlee used PayPal user's Banking Data to conduct "assessment[s]" in order to "improve[]" the "data quality" for "IAV").

³² ECF No. 492-40 at '050-051.

³³ ECF No. 365-5 at 10; ECF No. 178-39 at 55:12-18 (Vinay Raj testifying that "with PayPal," Yodlee does "use" the "stored credentials and MFA answers" to "refresh account details").

³⁴ *See* Declaration of Gary Olsen ("Olsen Report"), ECF No. 492-51 at Schedule 24 (); *see also supra* note 30.

³⁵ ECF No. 178-69 at '546 ("Ideally because this was a contractual obligation we should've built this [automatic purge feature] during PayPal implementation but since its way past that point now, we would need SUST to build this functionality.").

³⁶ Levis Decl. Ex. 11 at '902.

Yodlee knew it was not complying with its data-deletion obligations³⁷ and was “incorrectly stating what we do with IAV data.”³⁸ Multiple employees warned that Yodlee’s secret storage of PayPal users’ data was “extremely damaging,”³⁹ “will pose [] a compliance risk”;⁴⁰ “will be a huge concern to [PayPal’s] app security team”;⁴¹ “has the potential to blow up if not communicated properly”;⁴² and was an “MSA contractual breach that needs to be fixed.”⁴³ Yodlee silenced these employees, instructing them not to disclose Yodlee’s data-storage⁴⁴ and to only discuss it orally to avoid creating a written record.⁴⁵

Yodlee made further affirmative misrepresentations to PayPal regarding the deletion of PayPal users’ data. When Yodlee’s IAV contract was up for renewal in 2016, PayPal asked Yodlee to again confirm that its “data retention today is only 24 hours.”⁴⁶ After Yodlee falsely claimed it stored data for

³⁷ ECF No. 493-9 at ‘629 (Yodlee employees stating that Yodlee could not “request [] PayPal to delete as it is a contractual need that [Yodlee] perform[s] the purge” and that it would “lead to escalation and opening up a can of worms”); *id.* at ‘627 (Yodlee employees recognizing the “need” for a “permanent solution” to purge PayPal user data as it posed a “compliance risk” if PayPal “raises this in the future”); ECF No. 411-19 at ‘606 (stating that although a “[p]urge was supposed to be implemented at Yodlee” to delete PayPal user data, “nothing ha[d] been done on this”); ECF No. 493-21 at ‘542 (Yodlee employee circulating a screenshot of a database query showing that Yodlee was still maintaining data collected from more than 67 million PayPal accounts from 2014 to 2018 and warning that “we have data since 2014 for PAYPAL IAV+ cobrand”); ECF No. 493-8 at ‘973 (Yodlee’s previous Director of Application Security, Dheeraj Baht recognizing that “[t]here seems to be a discrepancy between PayPal’s [] belief and reality. PayPal doesn’t seem to be calling a Delete account API, and neither do we seem to be running a purge script”).

³⁸ ECF No. 493-19 at ‘903.

³⁹ ECF No. 493-7 at ‘803.

⁴⁰ ECF No. 493-9 at ‘627.

⁴¹ ECF No. 493-10 at ‘906.

⁴² ECF No. 493-11 at ‘654.

⁴³ ECF No. 493-9 at ‘628.

⁴⁴ ECF No. 493-8 at ‘973 (“Let’s be careful about what we say to PayPal about this. (Whether we have / haven’t been deleting)”; ECF No. 493-7 at ‘803 (“Let’s be clear on one thing . . . we have to be VERY careful about our messaging re: credentials. It was a PayPal InfoSec requirement that we did. The fact that we did not can be extremely damaging. I don’t want anything going out without me seeing / approving it first”); ECF No. 493-11 at ‘655 (“I haven’t had any conversations with [PayPal] on [Yodlee not purging the data] so far as guided by YSO earlier”); ECF No. 493-9 at ‘629 (“This is not the right time unfortunately to ask [PayPal] to implement purge API’s as it will lead to escalation and opening up a can of worms which we should avoid.”).

⁴⁵ ECF No. 493-8 at ‘973 (Yodlee employee urging others to “move [the discussion regarding not purging PayPal data] to a f2f or phone call interaction”).

⁴⁶ ECF No. 493-12 at ‘108.

just “24 hours,”⁴⁷ [REDACTED].⁴⁸ Consequently, [REDACTED]
 [REDACTED]⁴⁹ and
 remained under the false impression that Yodlee was “the clear winner [on data security] since they do
 not store bank credentials.”⁵⁰ The conduct described above is also reflected in Yodlee’s account-linkage
 data. [REDACTED]
 [REDACTED] Yodlee did
 [REDACTED]⁵²

F. PayPal’s Policies Did Not Disclose Yodlee’s Conduct

Given that Yodlee concealed its data practices from PayPal (*see* Section II.E), it is unsurprising
 that PayPal’s policies and terms did not disclose what Yodlee was truly doing with PayPal users’ data.

PayPal’s T&Cs—which [REDACTED] and, thus,
 only seen by Plaintiffs Szeto and Rollier⁵³—made incomplete and inaccurate statements, like [REDACTED]
 [REDACTED]⁵⁴ The T&Cs
 did not disclose that Yodlee would collect users’ Login Credentials and Banking Data, much less store
 that information indefinitely. As previously recognized by this Court (SJ Order at 19), PayPal’s Privacy
 Statement was equally insufficient to disclose Yodlee’s conduct, as it did not state Yodlee would collect
 and store PayPal users’ data and was [REDACTED], when

⁴⁷ *Id.* (stating on January 11, 2016 that Yodlee would respond to PayPal that “[the data retention period] would be 24 hours.”).

⁴⁸ ECF No. 492-21 at ‘651 ([REDACTED]).

⁴⁹ ECF No. 492-20 at ‘324.

⁵⁰ ECF No. 492-22 at ‘306.

⁵¹ *See* Olsen Report ¶¶ 64-65 ([REDACTED]); *id.* at Schedule 24 (same); *id.* at Schedule 17 (same).

⁵² *Id.* at Schedule 24 ([REDACTED]).

⁵³ Yodlee does not cite to any PayPal T&Cs post-2020. *See* Mot. 3-8; *see also* ECF No. 509-6 ¶¶ 17-20.

⁵⁴ *See* ECF No. 492-14 at ‘848 ([REDACTED]); ECF No. 492-15 at ‘857 (same); ECF No. 492-16 at ‘866 (same); *see also* ECF No. 509-6 ¶ 18 (PayPal’s declaration identifying these T&Cs as effective from October 2015 to June 2018).

1 Plaintiffs Cottrell, Lumb, and Clark linked accounts.⁵⁵ When it was hyperlinked after 2020,⁵⁶ it vaguely
 2 stated that PayPal may disclose user data to “service providers” to “perform services and functions at
 3 [PayPal’s] direction,” such as “verify[ing] your identity.”⁵⁷ It did not disclose that Yodlee would collect
 4 and store Login Credentials and Banking Data forever for its own use.

5 None of PayPal’s other policies or user agreements disclosed Yodlee’s data practices either. [REDACTED]
 6 [REDACTED], and there is no evidence any PayPal
 7 users (let alone Plaintiffs) would have seen or learned of them when they linked accounts using IAV.⁵⁸
 8 Moreover, these policies did not disclose Yodlee’s conduct. For example, PayPal’s March 29, 2017
 9 Privacy Policy stated that “[s]ervice [p]roviders” like Yodlee would “only use [users’] information in
 10 connection with the services they perform for [PayPal] and *not for their own benefit*.”⁵⁹ Similarly, the
 11 PayPal User Agreements in effect when Plaintiffs linked their bank accounts via IAV do not mention
 12 Yodlee and do not disclose that Yodlee would collect users’ Login Credentials and Banking Data.⁶⁰

13 **G. Yodlee Collected & Stored Plaintiffs’ Login Credentials and Banking Data**

14 Yodlee’s account linking data confirms [REDACTED]
 15 [REDACTED]⁶¹ Yodlee claims that it is unable to locate data collected
 16 from Plaintiff Szeto.⁶² However, PayPal’s record confirms that Plaintiff Szeto linked her bank account to

18 ⁵⁵ See Figures 2-3 [REDACTED] ECF No. 509-6 ¶ 24 (PayPal’s declaration
 19 stating the Privacy Statement was effective starting January 1, 2020).

20 ⁵⁶ ECF No. 509-6 ¶¶ 24-26 (PayPal’s declaration identifying PP_00008682, PP_00011891, and
 21 PP_00011902 as the PayPal Privacy Statements in effect when Plaintiffs Cottrell, Lumb, and Clark linked
 22 accounts).

23 ⁵⁷ See ECF No. 595-3 (PP_00008682 for Cottrell) at ‘686; *see also* ECF No. 595-4 (PP_00011891 for
 24 Lumb) at ‘897 (similarly stating that PayPal would share data with “[s]ervice providers” to help it
 25 “process[] payments”); ECF No. 595-5 (PP_00011902 for Clark) at ‘906, ‘912 (similar statements).

26 ⁵⁸ See *supra*, Figures 2 through 4 [REDACTED].

27 ⁵⁹ ECF No. 510-13 at ‘595 (emphasis added); *see also* ECF No. 510-14 (April 19, 2018 Privacy Policy
 28 vaguely stating PayPal may disclose user data to non-descript “service provider[s]” that “perform services
 and functions at [PayPal’s] direction”).

⁶⁰ See Levis Decl. Ex. 12 (user agreement in effect when Plaintiff Rollier linked account); Levis Decl. Ex
 13 (user agreement in effect when Plaintiff Szeto linked account); Levis Decl. Ex. 14 (user agreement in
 effect when Plaintiff Cottrell linked account). Yodlee does not cite the user agreements in effect when
 Plaintiffs Clark or Lumb linked accounts.

⁶¹ ECF Nos. 514-2 (Rollier), 512-5 (Cottrell), 512-6 (Lumb), 581-4 (Clark).

⁶² See ECF No. 553-2 (Yodlee’s Revised Opposition to Plaintiffs’ Motion to Certify Classes) at 5 n.4.

PayPal via IAV on May 20, 2018.⁶³ At this time, Yodlee’s customary IAV practice was to collect and store Login Credentials and Banking Data. *See* Section II.B. Yodlee does not claim that it deviated from this practice at any time, nor with regard to Plaintiff Szeto specifically.

III. LEGAL STANDARD

A court may grant summary judgment on a “claim or defense” only when there is “no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law.” Fed. R. Civ. P. 56(a). “In considering a motion for summary judgment, the court may not weigh the evidence or make credibility determinations, and is required to draw all inferences in a light most favorable to the non-moving party.” *Goins v. City & Cnty. of San Francisco*, No. 16-CV-06705, 2018 WL 10455157, at *2 (N.D. Cal. Mar. 20, 2018) (Kim, J.).

IV. ARGUMENT

A. Plaintiffs Have Article III Standing for Each Claim

To establish Article III standing, “a plaintiff must show, among other things, that the plaintiff suffered concrete injury in fact.” *TransUnion LLC v. Ramirez*, 594 U.S. 413, 417 (2021). Central to this inquiry is “whether the asserted harm has a ‘close relationship’ to a harm traditionally recognized” at common law, such as “intrusion upon seclusion.” *Id.* at 417, 425.⁶⁴

The Ninth Circuit has confirmed that examining, collecting, and storing another’s private information is a concrete harm sufficient for Article III standing because it bears a close relationship to the tort of intrusion upon seclusion. *See* SJ Order at 26 (recognizing the “loss of sensitive private information constitutes a ‘concrete and particularized’ injury sufficient for standing.”) (citing *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 598 (9th Cir. 2020)); *see also Jones v. Ford Motor Co.*, 85 F.4th 570, 574 (9th Cir. 2023) (holding collection and indefinite storage of “private communications” establishes Article III standing); *Sanchez v. Los Angeles Dep’t of Transp.*, 39 F.4th 548, 553 (9th Cir. 2022) (holding collection of location data conferred Article III standing); *Nayab v. Cap. One Bank (USA), N.A.*, 942 F.3d 480, 491 (9th Cir. 2019) (recognizing the “examin[ation]” of a “private

⁶³ ECF No. 492-35.

⁶⁴ At summary judgment, a Plaintiff is not required to prove “that they in fact have standing” but only that there is a “genuine question of material fact as to the standing elements.” *See Cent. Delta Water Agency v. United States*, 306 F.3d 938, 947 (9th Cir. 2002).

1 bank account” is an “intrusion upon seclusion” that has “long been actionable at common law” and would
 2 thus satisfy Article III); *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017) (“[v]iolations of
 3 the right to privacy have long been actionable” and do not require “additional consequences”).

4 Here, the evidence shows that Yodlee collected and stored each Plaintiff’s private Login
 5 Credentials, and then exploited that information to collect and store additional private Banking Data from
 6 their accounts. *See* Section II.B. This establishes Article III standing under Ninth Circuit precedent.

7 **i. Yodlee’s Collection of Transaction Data Is Irrelevant to Plaintiffs’ Standing**

8 Yodlee is incorrect that Plaintiffs lack Article III standing because it did not collect their
 9 Transaction Data. Mot. at 10. First, there is a material factual dispute over whether Yodlee collected
 10 Plaintiffs’ Transaction Data that must be resolved by a jury. *See* ECF No. 572-2 at 3-6 (outlining flaws in
 11 Yodlee’s purported “[e]vidence”). Second, none of Plaintiffs’ cause of action turn on the collection of
 12 Transaction Data, such that it could not be necessary to establish Article III standing for any claim.
 13 Yodlee’s additional claim-specific arguments fail for the reasons specified below:

14 **Invasion of Privacy.** Yodlee misstates that the Ninth Circuit’s decision in *Phillips*, which
 15 recognized that the “unlawful collection and storage” of private information confers Article III standing.
 16 *See* Mot. at 11 (citing *Phillips v. U.S. Customs & Border Prot.*, 74 F.4th 986 (9th Cir. 2023)). In *Phillips*,
 17 the Ninth Circuit reaffirmed that the “retention of records” constitutes an Article III injury when it is
 18 alleged that the records were private or acquired through means that violate the right to privacy—both of
 19 which Plaintiffs allege here.⁶⁵ *Id.* at 994 (citing *Norman-Bloodsaw v. Lawrence Berkeley Lab’y*, 135 F.3d
 20 1260, 1264 (9th Cir. 1998) (finding “unauthorized obtaining” of the records “itself” established harm
 21 because the records were inherently private); *id.* (citing *Mayfield v. United States*, 599 F.3d 964, 970 (9th
 22 Cir. 2010) (holding standing was established “by the very fact of [continued] retention” because records
 23 were obtained in violation of privacy rights). *Phillips* did not require Plaintiffs to go beyond these concrete
 24 privacy injuries, such as by showing an out-of-pocket loss or that their data is lost, or no longer valuable,
 25 as Yodlee argues. Mot. at 11. Yodlee’s argument is also belied by the Ninth Circuit’s decision in *Jones*
 26

27 ⁶⁵ Here, Plaintiffs establish both: (1) their Login Credentials and Banking Data are inherently private; and
 28 (2) the means by which Yodlee acquired this data (i.e., secretly obtaining and storing their Login
 Credentials and then crawling around their bank accounts) is a privacy violation.

two months after *Phillips*, which again reaffirmed that collecting and storing private data confers Article III standing. *See Jones*, 85 F.4th at 574 (explaining the “relevant law is settled” and the collection and storage of “private communications” by itself establishes Article III standing).

Yodlee also argues that Plaintiffs lack Article III standing because the data it collected from them was supposedly “encrypted” and “securely stored.” Mot. at 11. This is irrelevant. *Id.* Whether Yodlee takes precautions to prevent *other* third parties from acquiring Plaintiffs’ data from itself does not negate the privacy harms caused by Yodlee’s own acquisition, storage, and use of that private information. Not surprisingly, Yodlee cites no authority supporting this proposition. *Id.*

Finally, Yodlee erroneously relies on Plaintiffs’ *class-wide* damages models to argue that Plaintiffs were not individually harmed by its retention of Login Credentials and Banking Data because those models do not quantify *monetary damages* for that misconduct. Mot. at 11-12. But Article III is not this narrow, and also allows standing based on “intangible,” non-monetary harms like privacy violations. *TransUnion LLC*, 594 U.S. at 417 (explaining standing encompasses “intangible harms”); *Brown v. Google LLC*, 685 F. Supp. 3d 909, 923-24 (N.D. Cal. 2023) (holding that defendant’s “collection and storage” of plaintiffs’ data result in “‘intangible’ but concrete harms” sufficient to give rise to standing). Thus, even if Yodlee were correct about Plaintiffs’ damages models, Plaintiffs would still have Article III standing to pursue claims based on Yodlee’s taking of their Login Credentials and Banking Data. In any event, Plaintiffs *are* seeking monetary damages based on Yodlee’s taking of Login Credentials and Banking Data in the form of (1) statutory damages under CAPA, which do not require the collection of Transaction Data (*see* Section IV.C), and (2) nominal damages for invasion of privacy based exclusively on “Yodlee’s collection and storage of [Login] Credentials.” *See* Olsen Report ¶¶ 10-16.⁶⁶

CAPA. Yodlee’s assertion that Plaintiffs must allege “additional consequences” beyond a violation of CAPA to establish Article III standing is also incorrect. CAPA was enacted to prevent the unauthorized collection of “identifying data” through phishing. Comm. Rep. Cal. S.B. 355 (Apr. 8, 2005), 2005 WL 1907987 (intending to combat the “technique for obtaining personal information” through

⁶⁶ Yodlee’s reliance on cases involving future risk of harm are distinguishable because the privacy harms it caused have already occurred. *See* Mot. at 11-12 (citing *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (evaluating future risk of harm); *I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034, 1050 (N.D. Cal. 2022) (same)).

1 fraudulent websites to instill “[c]onfidence in the integrity of personal information transmitted via the
 2 Internet.”). CAPA thus protects a substantive right to privacy, i.e., the right to control one’s private
 3 “identifying information” on the internet. *Facebook Tracking*, 956 F.3d at 598 (explaining “right to
 4 privacy” includes the “individual’s control of information concerning his or her person.”) (internal citation
 5 omitted). Because a violation of CAPA harms this substantive right, a violation of CAPA independently
 6 establishes Article III standing. *Eichenberger*, 876 F.3d at 983-84 (explaining where a violation infringes
 7 on the “substantive right to privacy” that a “Plaintiff need not allege any further harm”).

8 Yodlee erroneously relies on a single out-of-district decision, *Lawrence v. Finicity Corp.*, to argue
 9 that CAPA requires “additional consequences” for Article III standing. Mot. at 12 (citing 716 F. Supp. 3d
 10 851, 872 (E.D. Cal. 2024)). *Lawrence* is inapposite and should be disregarded because the court incorrectly
 11 assumed CAPA was a purely procedural statute and thus misapplied its Article III standing analysis. *See*
 12 *Lawrence*, 716 F. Supp. 3d at 871-72. Even so, Plaintiffs here suffered “additional consequences” because
 13 Yodlee used the Login Credentials it obtained in violation of CAPA to gather *additional* Banking Data
 14 from Plaintiffs’ accounts. *See* Section II.B. This further “intrusion upon [Plaintiffs’] financial accounts”
 15 constitutes “additional consequences” sufficient for Article III standing even under *Lawrence*. 716 F.
 16 Supp. 3d at 871.

17 **Unjust Enrichment.** Yodlee’s claim that Plaintiffs’ unjust enrichment claim solely relates to
 18 Yodlee’s use of Transaction Data (Mot. at 10-11) ignores Plaintiffs’ actual allegations and the record
 19 evidence substantiating them. *See* Complaint ¶¶ 145, 150 ([REDACTED]
 20 [REDACTED]
 21 [REDACTED]; *see also* Section II.D (describing Yodlee’s use of PayPal IAV data). Because Yodlee was
 22 unjustly enriched by Plaintiffs’ Login Credentials and Banking Data, whether Yodlee also collected their
 23 Transaction Data is irrelevant to their Article III standing.

ii. Plaintiffs Lumb and Clark Have Standing

Yodlee claims that Plaintiffs Lumb and Clark “manufactured” standing. Mot. at 10. This is wrong.⁶⁷ Mot. at 10. Both Plaintiffs have submitted sworn testimony that they linked financial accounts as early as [REDACTED], well in advance of joining this lawsuit.⁶⁸ While Yodlee claims its data shows they only linked accounts through IAV in December 2022 and April 2023 (ECF No. 492-35), respectively, this only confirms they have standing because Yodlee did, in fact, collect, store, and use their Login Credentials and Banking Data.

B. Plaintiffs May Bring Claims Under California Law

Plaintiffs’ claims are governed by California law because virtually (if not) all of the illegal conduct underlying their claims occurred in California, where Yodlee and PayPal were based and where Yodlee collected, stored, and exploited Plaintiffs’ data. *See* Section II.A.; *see also Mazza v. Am. Honda Motor Co.*, 666 F.3d 581, 592 (9th Cir. 2012) (“[California] has ‘the predominant interest’ in regulating conduct that occurs within its borders.”).

Yodlee has not identified any state with an interest in regulating claims occurring within California’s borders. *See Opperman v. Path, Inc.*, No. 13-CV-00453-JST, 2016 WL 3844326, at *10 (N.D. Cal. July 15, 2016) (applying California nationwide where defendants failed to identify other state’s interests).⁶⁹ Instead, Yodlee argues that the law of each Plaintiff’s home state applies because this is where they viewed the misrepresentations in the IAV interface.⁷⁰ Mot. at 13-14. This is wrong. In evaluating which state’s law should apply, California courts look to the place where the last act necessary to complete

⁶⁷ Yodlee also notes that Plaintiff Cottrell continued “using” his “IAV linked account” after joining this lawsuit. Mot. at 7 n.1. This is immaterial because his Login Credentials and Banking Data were already collected and stored by Yodlee without his consent.

⁶⁸ *See* ECF No. 178-82 at 19 (Plaintiff David Lumb’s Amended Responses and Objections To Defendant Yodlee Inc.’s First Set Of Interrogatories To Plaintiffs); *id.* at 7-8 (Plaintiff Darius Clark’s Amended Responses and Objections To Defendant Yodlee Inc.’s First Set Of Interrogatories To Plaintiffs).

⁶⁹ Yodlee *generally* claims state laws vary by relying on its Revised Opposition to Plaintiffs Motion to Certify Classes. *See* Mot. at 13 (citing ECF No. 553-2 at 10:12-11:28). Plaintiffs have already explained previously there are no material differences between California and other states’ privacy laws. *See* ECF No. 561-2 (Plaintiffs’ Revised Reply in Support of Motion to Certify Classes) at 6.

⁷⁰ At a minimum, Plaintiff Szeto is a California resident. *See* ECF No. 514-5 at 4. While Yodlee claims she used IAV when she was in Georgia, the evidence it cites does not support this. Mot. at 14. At best, Yodlee has evidence that Plaintiff Szeto attended trainings in Georgia for a “couple weeks” sometime between May 1, 2018 and September 2018. *See* Mot. at 14 (citing ECF No. 510-3 at 27:20-28:20).

1 the claim occurs. *Mazza*, 666 F.3d at 593. Here, none of Plaintiffs' claims are completed by viewing
 2 screens in their home states, because, as set forth below, they require additional misconduct by Yodlee
 3 that took place in California.

4 **CAPA.** Plaintiffs' CAPA claim accrued when Yodlee completed collecting Plaintiffs' Login
 5 Credentials over the internet. *Cottle v. Plaid Inc.*, 536 F. Supp. 3d 461, 492 (N.D. Cal. 2021) (explaining
 6 an individual is "adversely affected" under CAPA when the defendant "obtained their identifying
 7 information" and "used that information"). This occurred in California, where Yodlee performed the
 8 collection and stored Plaintiffs' Login Credentials. *See* Sections II.A-B. Yodlee cannot avoid this
 9 conclusion by analogizing CAPA to run-of-the mill consumer fraud statutes like those at issue in *Mazza*.
 10 Mot. at 13-14 (citing *Lawrence*, 716 F. Supp. 3d at 871). Unlike traditional consumer fraud, where the
 11 "last act" occurs at the place plaintiffs purchased defective or deceptively labeled goods, CAPA prohibits
 12 the collection of specific types of "identifying information" by deceit via Yodlee's servers and personnel
 13 in California, not in Plaintiffs' home states. *See* Cal. Bus. & Prof. Code §§ 22948.1-22948.2. Thus, where
 14 Plaintiffs encountered Yodlee's account linking screens are irrelevant because that is not the "place where
 15 the last act" needed to pursue CAPA claims occurred. *See Mazza*, 666 F.3d at 593.

16 **Privacy Claims.** Plaintiffs' privacy claims became complete when (1) Yodlee collected and stored
 17 their Login Credentials; and (2) used those Login Credentials to access their private bank accounts to
 18 collect additional Banking Data. Both acts occurred [REDACTED] where Yodlee's "agents" collect this
 19 data and where Yodlee [REDACTED] and uses it for its own benefit.⁷¹ *See Opperman*, 2016 WL
 20 3844326, at *8, 11 (finding California common law intrusion appropriately applies to non-residents where
 21 "all data held by [the defendant]" was "managed by [defendant's] employees" in California). Yodlee's
 22 citation to *Katz-Lacabe v. Oracle Am., Inc.*, 668 F. Supp. 3d 928, 948 (N.D. Cal. 2023) further supports
 23 applying California law to Plaintiffs' claims, albeit on different grounds. *Katz* found the "last event[]" for
 24 the plaintiffs' data collection privacy claims occurred where "third-party websites" decided to use the
 25

26 ⁷¹ *See* ECF No. 178-43 at 4 (explaining Yodlee's "[a]gents" are "capable of navigating to different web
 27 pages and retrieving data to be displayed to the consumer on the partner's website"); ECF No. 518-7 at
 28 17 ([REDACTED]); *see also* Section II.A [REDACTED]

defendant's offending software. *Id.* To the extent *Katz* is applicable here, the relevant "last act" would occur in California, where PayPal is headquartered and incorporated Yodlee's software.⁷²

Unjust Enrichment. Finally, Plaintiffs' unjust enrichment claims materialize when Yodlee unjustly benefitted from Plaintiffs' data. This too, occurred in California, where Yodlee uses Plaintiffs' Login Credentials and Banking Data for its own benefit. *Chinacast Educ. Corp. v. Chen Zhuoguo*, No. CV 15-05475-AB (EX), 2018 WL 6074551, at *5-6 (C.D. Cal. Sept. 7, 2018) (holding "last act" for unjust enrichment is where property was "received" and where defendant "wrongfully exercised dominion over" such property). While Yodlee again relies on *Mazza*, (Mot. at 13) that decision is distinguishable because Plaintiffs' unjust enrichment claims are not based on typical consumer fraud.⁷³

C. Plaintiffs' CAPA Claims Should Proceed

CAPA prohibits any person from "induc[ing] another person to provide identifying information by representing itself to be a business without the authority or approval of the business." Cal. Bus. & Prof. Code § 22948.2. "Identifying information" includes a "[a]ccount passwords" and "[a]ny other piece of information that can be used to access an individual's financial accounts." *Id.* § 22948.1(b). Anyone whose "identifying information" is taken and "adversely affected" may bring a CAPA claim. *Id.* § 22948.3(a)(2). Yodlee violated CAPA when it posed as Plaintiffs' banks, using fake login portals, to collect their Login Credentials, and then used those credentials to collect further Banking Data from their accounts. *See* Section II.B. The Court upheld these allegations when Yodlee first moved for summary judgment, holding that "a reasonable person could interpret the [false login portal], to be a direct link to their bank's website," and Plaintiffs were "adversely affected because their financial data was taken when Yodlee allegedly mimicked their banks' websites." SJ Order at 17, 26.

⁷² *See* ECF No. 178-68 at '807

Yodlee's citation to *In re Yahoo Mail Litig.*, 308 F.R.D. 577, 605 (N.D. Cal. 2015) is of no moment. That case involved CIPA, which the California legislature has "specifically stated" is only intended to "protect the right of privacy of the people of this state." *Id.* The same is not true for common law invasion of privacy claims.

⁷³ Separately, even if Yodlee could show other states have an interest in Plaintiffs' claims (which they do not) Yodlee fails to show this interest would be greater than California's.

Hoping to avoid liability, Yodlee now proffers a series of irrelevant “defenses” concerning its own legitimacy as a company, whether it acted at PayPal’s direction, whether it committed identity theft, and whether it provided a benefit to Plaintiffs. Mot. at 15. None is a basis for summary judgment. Its other arguments, below, also fail.

i. Yodlee Represented Itself as Financial Institutions Without Approval

Yodlee violated CAPA when it collected Plaintiffs’ data through a false login portal that mimicked a direct login portal to their banks. To reinforce the perception that users were connecting to their banks, Yodlee surrounded the false login portal with banks’ names, along with logos or URLs, in addition to language that described the portal as a “bank login” and instructions to “Log in to your online banking.” See Section II.C.

Yodlee raises three arguments for why its use of false bank login portals was not an illegal “misrepresentation” under CAPA, all of which fail.

First, Yodlee points to language on the portal stating that the purpose of entering credentials is to “link” a financial account and that the portal also included PayPal’s logos. Mot. at 16. Both are irrelevant. What matters is that Yodlee falsely represented that the account linking would occur by users “log[ging]” into their bank accounts, and not by providing their Login Credentials to Yodlee. See Sections II.B-C.

Second, Yodlee notes that the post-2020 screens used by Cottrell, Clark, and Lumb mention that PayPal “use[s] Yodlee to confirm your bank details and to check your balance and transactions as needed, which can help your PayPal payments go through.” Mot. at 8. Yodlee already raised this argument and lost. SJ Order at 17, 26. As the Court previously held, this passing mention of Yodlee does not negate that the false login portal appeared to be “a direct link to their bank’s website.” *Id.* at 17. Indeed, nothing in this statement would alert PayPal users that the portal presented to them—with their bank logo and instructions to “[l]og in”—was not operated by their bank. See Section II.F.⁷⁴

Third, Yodlee argues that the deceptive nature of the false login portal was authorized by language buried in PayPal’s T&Cs. Mot. at 16. Not so. Yodlee does not identify any language that would have put

⁷⁴ Plaintiffs repeat that the Court’s determination on the merits that PayPal users knew or “obviously understand” Yodlee’s role in the account linking process was error at class certification, and would be error now, because this is a jury issue. See ECF No. 600 at 7.

Plaintiffs on notice that the bank login portal was fake and connected to Yodlee, or authorized Yodlee's indefinite storage and use of their data. *See* Section II.F. Yodlee's conduct is not comparable to the two cases it cites, which (1) did not involve CAPA claims; and (2) involved instances where reasonable minds could not differ because the alleged defamatory or misrepresenting statement was obviously non-actionable. Mot. at 15 (citing *Knieval v. ESPN*, 393 F.3d 1068, 1076 (9th Cir. 2005) (dismissing defamation claim because statement that Mr. Knieval is a "pimp" was a clear joke not intended to imply he engaged in criminal behavior); *Sponchiado v. Apple Inc.*, No. 18-CV-07533-HSG, 2019 WL 6117482, at *4 (N.D. Cal. Nov. 18, 2019) (dismissing alleged visual misrepresentation of screen size based on "obvious language" that was not "inconspicuous" in the advertisement disclosing the screen was smaller than shown)).

ii. Plaintiffs Were Adversely Affected under CAPA

Like other statutes, CAPA's "adversely affected" language reflects a statutory "standing" requirement—unrelated to Article III standing—that authorizes individuals whose identifying information is obtained through phishing to bring a private right of action. *See, e.g., Citizens for Better Forestry v. U.S. Dep't of Agric.*, 341 F.3d 961, 976 (9th Cir. 2003) (explaining statutory standing requires a "legal wrong" or "injury" that falls within the "zone of interests" the statute protects); *see also E. Bay Sanctuary Covenant v. Trump*, 932 F.3d 742, 768 (9th Cir. 2018) (explaining the "zone of interests" test for statutory standing is not "especially demanding"). Because each Plaintiff had their identifying information taken online through deceit—the precise zone of interest protected by CAPA—each Plaintiff was "adversely affected" and has statutory standing to pursue these claims. *See Cottle*, 536 F.Supp.3d at 492 (holding plaintiffs' allegations that their bank credentials were harvested through fake bank login screens were sufficient to meet CAPA's "adversely affected" requirement).

Yodlee's argument that Plaintiffs must prove "additional consequences" (Mot. at 17 (citing *Lawrence*, 716 F. Supp. 3d at 871)) contradicts CAPA's plain text and this Court's prior SJ Order.⁷⁵ *See Lopez v. Contra Costa Reg'l Med. Ctr.*, No. C 12-03726 LB, 2014 WL 4349080, at *4 (N.D. Cal. Sept. 2,

⁷⁵ Yodlee's assertion that "[s]ubsequent developments" in the record require overturning this Court's prior SJ Order is baseless. Mot. at 16. Pointing to the absence of certain types of evidence (i.e., testimony) does not change that a material dispute exists.

2014) (courts may not “insert[] language the Legislature did not put in the legislation.”); *see also* SJ Order at 26 (holding the fact that Plaintiffs’ “financial data was taken when Yodlee allegedly mimicked their banks’ websites” was “sufficient to show” they were adversely affected). Regardless, Plaintiffs suffered additional consequences when Yodlee took their Login Credentials, as Yodlee then used the credentials to collect additional Banking Data from their accounts. *See* Section II.B. That Plaintiffs did not affirmatively testify they were “induce[d],” or do not remember the exact screens they viewed years ago, does not affect the uncontroverted evidence that Yodlee collected Plaintiffs’ identifying information through a false login portal. Mot. at 17.

iii. Yodlee Directly Violated CAPA

It is indisputable that Yodlee “directly” violated CAPA. Mot. at 17. Yodlee created, designed, and operated IAV, including the account-linking screens each Plaintiff encountered, which it used to induce them to hand over their Login Credentials, and ultimately collect additional Banking Data. *See* Sections II.B-C.

Yodlee’s assertion that it was actually PayPal who “designed” and “customized” the account-linking screens is belied by the record. Mot. at 18.⁷⁶ [REDACTED] that Yodlee’s clients integrate into their existing apps and website to avoid having to build a comparable system from scratch.⁷⁷ This is why the account-linking screens in the PayPal app closely mirror the account-linking screens of other apps using IAV.⁷⁸ Yodlee’s customers, including PayPal, cannot and do not customize the screens in the manner Yodlee contends, [REDACTED]. *See* Section II.C. Even if PayPal could customize the user interface, it does not change that it was *still Yodlee* who controlled, used, and implemented the account-linking screens to induce Plaintiffs to provide their Login Credentials. *Id.* Yodlee’s citations to *Warner* and *Prasad* confirm Yodlee acted “directly” in this case. Mot. at 17-18 (citing *Warner v. Experian Info. Sols., Inc.*, 931 F.3d 917, 921 (9th Cir. 2019) (no

⁷⁶ It is irrelevant who “hosted” the account-linking screens, i.e., whether it was Yodlee or PayPal providing the actual servers for that part of the interface at any given time (Mot. at 18), because it was Yodlee who created, provided, and designed the account-linking screens and ultimately sought to induce Plaintiffs and all PayPal users to hand over their Login Credentials in violation of CAPA.

⁷⁷ *See* Levis Ex. 15 at 27:18-28:22 ([REDACTED]).

⁷⁸ ECF No. 178-24 (E-Trade IAV log-in screen); ECF No. 178-23 (Charles Schwab IAV login screen); ECF No. 178-25 (Amazon IAV log-in screen).

liability because, unlike here, defendant did not “review” the offending letter and played “no role” in preparing its “contents”); *United States v. Prasad*, 18 F.4th 313, 325 (9th Cir. 2021) (finding “directly” requirement satisfied when defendant “exercise[d] . . . control”).

iv. Plaintiffs Rollier & Szeto’s CAPA Claims Are Not Time-Barred

Yodlee’s statute of limitations defense fails because Plaintiffs Rollier and Szeto did not know, and had no way to discover, that Yodlee was impersonating their financial institutions to obtain their Login Credentials or Banking Data when they linked their accounts. *See* Section II.F; *see also Cain v. State Farm Mut. Auto. Ins. Co.*, 62 Cal. App. 3d 310, 315 (Cal. Ct. App. 1976) (holding that the discovery rule applies to “violation of the right of privacy”); *SkinMedica, Inc. v. Histogen Inc.*, 869 F. Supp. 2d 1176, 1199 (S.D. Cal. 2012) (finding “a genuine issue of material fact” exists as to application of the discovery rule where defendant’s “misappropriation was surreptitious” and plaintiff “could not and did not discover” the misconduct); *San Diego Cnty. Credit Union v. Citizens Equity First Credit Union*, No. 18CV967-GPC(MSB), 2020 WL 5797826, at *5 (S.D. Cal. Sept. 29, 2020) (finding that the discovery rule applies where plaintiff was “not aware of” defendant’s misconduct until a later time).

The cases Yodlee cites in support of its statute-of-limitations defense are inapposite, as they involve principles only applicable to mortgage and loan cases or instances where the evidence established the plaintiff had actual knowledge of her claim, which Plaintiffs did not have here. Mot. at 18-19 (citing *Fowler v. Univ. of Phoenix, Inc.*, 817 F. App’x 442, 443 (9th Cir. 2020) (no tolling because plaintiff made “frequent assertions” confirming knowledge of her claim); *Marsicano v. Bank of Am. N.A.*, No. CV166189, 2016 WL 10968664, at *3 (C.D. Cal. Dec. 19, 2016) (explaining in “mortgage- and loan-related cases” failure to “read loan documents” that disclose the conduct does not toll statutes of limitation)).

D. Plaintiffs’ Privacy Claims Should Proceed

Yodlee’s unauthorized collection and storage of Plaintiffs’ Login Credentials and Banking Data establishes claims for invasion of privacy. *See* SJ Order at 16-18. Plaintiffs have a well-recognized expectation of privacy in private financial information like Login Credentials and Banking Data. *See Wesch v. Yodlee, Inc.*, No. 20-CV-05991, 2021 WL 1399291, at *3 (N.D. Cal. Feb. 16, 2021) (holding Yodlee violates Plaintiffs’ reasonable expectation of privacy by “access[ing] and retain[ing] their

personal, financial accounts”); *Taus v. Loftus*, 40 Cal. 4th 683, 732 (Cal. 2007) (recognizing that improperly obtaining and “examin[ing] the bank’s records of[a person’s] account” violates that personal’s reasonable expectation of privacy and constitutes intrusion upon seclusion). Yodlee’s collection, storage, and use of Plaintiffs’ Login Credentials and Banking Data is highly offensive to a reasonable person. *See* SJ Order at 17-18 (holding that a jury could find it highly offensive that Yodlee obtained users’ login credentials and accessed their financial data through deceptive means, and that Yodlee stored the credentials indefinitely); *see also Nayab*, 942 F.3d at 491 (holding that “examining [a] private bank account” is an “invasion” sufficient for an intrusion upon seclusion claim.).

i. Yodlee’s Conduct Is Highly Offensive

Yodlee argues that its data-practices were not highly offensive because it did not collect Plaintiffs’ Transaction Data, only their Login Credentials and Banking Data. Mot. at 22-24. This argument fails. First, whether Yodlee collected, stored, and used/monetized Plaintiffs’ Transaction Data is a disputed issue. *See* Section IV.A.i. Second, Yodlee collected, stored, and used Plaintiffs’ Login Credentials and Banking Data, which is itself highly offensive. *See* SJ Order at 17-18 (finding that Yodlee’s collection and indefinite storage of users’ login credentials and financial data would be highly offensive if they are not necessary for “complet[ing] the transaction”). That statutes like CAPA protect the collection of Login Credentials and Banking Data underscores its offensiveness. At a minimum, this is a fact question for the jury that cannot be resolved on summary judgment. *See Opperman*, 205 F. Supp. 3d at 1080 (finding highly offensiveness is an issue that should be left to “a jury or legislature” to “reflect[] the community’s standards as they relate to the privacy of information” and a judge “should be cautious before substituting his or her judgment for that of the community”); *Virgil v. Time, Inc.*, 527 F.2d 1122, 1131 (9th Cir. 1975) (holding that whether conduct is “highly offensive to a reasonable person” cannot be decided as a matter of law when “reasonable minds . . . differ”).⁷⁹

The only cases Yodlee cites where the offensiveness was resolved before trial involved far less sensitive types of information, like anonymous app usage statistics, or social media profile URLs, where

⁷⁹ Yodlee’s claim that it does delete the data when requested by PayPal (Mot. at 23) is incompatible with the record. *See* Sections D-E. Its claim that PayPal knew it was storing credentials after January 2019 or wanted it to do so has no bearing on whether this conduct is offensive to PayPal users. Mot. at 23.

the conduct was not offensive. *See* Mot. at 22 (citing *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 286-87 (Cal. 2009) (expectation of privacy in the workplace); *Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1088 (N.D. Cal. 2022) (disclosure mobile app usage statistics); *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) (collection of LinkedIn profile URLs); *Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (Cal. Ct. App. 2011) (collection of address information to send mailed coupons); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (disclosure of geolocation data); *Yunker v. Pandora Media, Inc.*, No. 11-CV-03113, 2013 WL 1282980, at *14-15 (N.D. Cal. Mar. 26, 2013) (noting PII, by itself, was not highly offensive but may have been if transmitted alongside “sensitive financial information . . . or passwords”). The data here is far more private.⁸⁰

ii. Yodlee Did Not Obtain Plaintiffs’ Consent

Almost two years have passed since Yodlee’s first unsuccessful attempt at summary judgment (*see* SJ Order at 18-19), Yodlee still fails to meet its burden to show that Plaintiffs consented to the collection, indefinite storage, and use of their Login Credentials and Banking Data.

Account Linking Screens. The Court has already considered and rejected Yodlee’s argument that the account linking screens establish consent. *See* SJ Order at 18-19. Nothing has changed since that ruling, and Yodlee no longer argues these screens establish consent. Mot. at 20 (relying exclusively on PayPal’s hyperlinked terms).

PayPal’s Policies. PayPal’s T&Cs, Privacy Statement, and other various, non-linked policies do not establish consent either. Not only were these terms unavailing within the account-linking interface at times when Plaintiffs linked their accounts to PayPal (*see* Sections II.B&F), but these terms do not disclose that Yodlee will collect, store, and use PayPal users’ Login Credentials or Banking Data. *Id.* For instance, the T&Cs linked to the account flows merely state Yodlee may “receive information requested by you.” *Id.* Neither these non-descript terms nor any of PayPal’s other policies are sufficient to establish actual and specific consent for the intrusive conduct at issue in this case. *See Van Patten v. Vertical Fitness Group, LLC*, 847 F.3d 1037, 1045 (9th Cir. 2017) (holding consent for certain “communications” does not mean “that the consumer consents to any and all contact.”); *Opperman*, 205 F. Supp. 3d at 1072

⁸⁰ Plaintiffs allege injury or harm for the reasons stated in Section IV.A.i.

(explaining consent is limited to the “particular conduct” disclosed); *Golan v. Veritas Entertainment*, No. 4:14-cv-00069 ERW, 2017 WL 2861671, at *8 (E.D. Mo. July 5, 2017) (holding “consent for one purpose does not equate to consent for all purposes”). The Court’s factual finding on class certification that PayPal users “understand” Yodlee’s role is inconsistent with this case law and what was actually disclosed to PayPal users. Mot. at 20 (citing ECF No. 600).

User Permissions. Yodlee’s argument that Cottrell and Szeto’s “permissions” screens state they permitted PayPal to check their accounts *after* linking to IAV fails for two reasons. Mot. at 21. First, consent does not apply retroactively so it is wholly irrelevant what these post-account linking screens may convey. See SJ Order at 19 (citing *Opperman*, 205 F. Supp. 3d at 1007, n.8). And, separately, these permissions screens—like the account linking flow—do not mention Yodlee at all and refer exclusively to permissions “given to PayPal[.]” See ECF Nos. 514-10 at ‘010, 514-11 at ‘005.⁸¹

Yodlee relies on cases that involve clear disclosures—for the collection of innocuous data—that are inapposite to the vague and ambiguous terms it claims establish consent to the collection of private Login Credentials and Banking Data here. Mot. at 19-21 (citing *Hammerling v. Google LLC*, No. 22-17024, 2024 WL 937247, at *1 (9th Cir. Mar. 5, 2024) (finding Google had consent to collect certain app usage data from its own operating system because Google’s policy stated it collected information from “app[s]” that use its “operating system”); *Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 955 (N.D. Cal. 2017), *aff’d*, 745 F. App’x 8 (9th Cir. 2018) (finding users consented to tracking on third-party websites because Facebook disclosed it would “collect information when you visit or user third-party websites”); *Silver v. Stripe Inc.*, No. 4:20-CV-08196, 2021 WL 3191752, at *3 (N.D. Cal. July 28, 2021); *Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1213 (N.D. Cal. 2014) (finding consent to obtain email addresses because disclosure stated it would collect information from “your . . . [email address]” including “Google contacts”); *Javier v. Assurance IQ, LLC*, No. 4:20-CV-02860, 2021 WL 940319, at *2, 4 (N.D. Cal. Mar. 9, 2021) (finding consent to collect information, including name of bank/card issuer, time of purchase, and whether consumer had sufficient funds, because policy stated collected information included “credit card data” “commercial information” and “relevant order information”); *Hart v. TWC Prod. & Tech. LLC*,

⁸¹ This refutes Yodlee’s assertion that PayPal users can “turn off” the use of Yodlee through account permissions. Mot. at 3. PayPal users cannot turn off a service that is not listed.

No. 20-CV-03842, 2023 WL 3568078, at *11 (N.D. Cal. Mar. 30, 2023) (finding consent barred certification because it was “undisputed” the policy “explicitly disclosed the practices at issue”); *Heldt v. Guardian Life Ins. Co. of Am.*, No. 16-CV-885, 2019 WL 651503, at *5 (S.D. Cal. Feb. 15, 2019) (finding consent to share health data because plaintiff signed authorization for processing insurance claim that stated “medical and/or income data” will be “release[d]” to assess the claim). These examples (if anything) confirm that the account-linking screens and terms and conditions within the PayPal user interface fall short of providing the specificity needed to establish consent for Yodlee’s collection, storage, and use of Plaintiffs Login Credentials and Banking Data here.

E. Plaintiffs’ Unjust Enrichment Claims Should Proceed

The Court previously denied Yodlee’s Motion for Summary Judgment on Plaintiffs’ unjust enrichment claims. *See* SJ Order at 24-25. Yodlee claims dismissal is proper *now* because it *again* claims it did not sell or use Plaintiffs’ Transaction Data. Mot. at 24-25. This remains a disputed fact. *See* ECF No. 492-5 at 13-14; ECF No. 572-2 at 3-6. But regardless, record evidence shows Yodlee used PayPal IAV data for its own benefit, separate and apart from whether it used and profited from PayPal IAV users’ transactions. *See* Section II.D. Because Yodlee does not and cannot dispute this evidence, summary judgment on Plaintiffs’ unjust enrichment claims would be improper. *Swafford v. Int’l Bus. Machines Corp.*, 408 F. Supp. 3d 1131, 1150 (N.D. Cal. 2019) (holding that “genuine issue[]” of whether defendant committed the underlying wrongdoing meant a “genuine issue[]” also existed “as to whether or not it would be unfair or unjust for [defendant] to retain the benefit . . . conferred on it.”).⁸²

V. CONCLUSION

For the foregoing reasons, Yodlee’s Motion should be denied in its entirety.

Dated: November 8, 2024

/s/ Christian Levis

Christian Levis (admitted *pro hac vice*)

Margaret MacLean (admitted *pro hac vice*)

Amanda Fiorilla (admitted *pro hac vice*)

LOWEY DANNENBERG, P.C.

44 South Broadway, Suite 1100

White Plains, New York 10601

Telephone: (914) 997-0500

⁸² Yodlee’s argument that Plaintiffs’ individual claims fail under other state laws (Mot. at 19, 24) is irrelevant because Plaintiffs did not bring these claims.

Facsimile: (914) 997-0035
clevis@lowey.com
mmaclean@lowey.com
afiorilla@lowey.com

Anthony M. Christina (admitted *pro hac vice*)
LOWEY DANNENBERG, P.C.
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, Pennsylvania 19428
Telephone: (215) 399-4770
Facsimile: (914) 997-0035
achristina@lowey.com

Benjamin Steinberg (admitted *pro hac vice*)
SHINDER CANTOR LERNER LLP
14 Penn Plaza, 19th Floor
New York, NY 10122
Telephone: (646) 960-8601
Facsimile: (646) 960-8625
benjamin@scl-llp.com

John Emerson (admitted *pro hac vice*)
EMERSON FIRM, PLLC
2500 Wilcrest Drive, Suite 300
Houston, TX 77042
Telephone: (800) 551-8649
Facsimile: (501) 286-4659
jemerson@emersonfirm.com

Robert Kitchenoff (admitted *pro hac vice*)
WEINSTEIN KITCHENOFF & ASHER LLC
150 Monument Road, Suite 107
Bala Cynwyd, PA 19004
Telephone: (215) 545-7200
kitchenoff@wka-law.com

Michele Carino (*pro hac vice* forthcoming)
GREENWICH LEGAL ASSOCIATES LLC
881 Lake Avenue
Greenwich, CT 06831
Telephone: (203) 622-6001
Mcarino@grwlegal.com
*Attorneys for Plaintiffs and the Proposed
Classes*